DATASHEET

CRITICAL**START**® Cyber Operations Risk & Response™ Platform

Providing end-to-end cybersecurity visibility to reduce risk.

KEY BENEFITS

- ✓ **Efficient Risk Management**
  Manage and track the lifecycle of Risk-Ranked Reduction Recommendations spanning Critical Start service offerings and your other security programs for a single view of cyber risk
- ✓ **Unified Dashboard**
  See your Risk Assessments, Asset Visibility, and Managed Detection and Response (**MDR**) results and metrics in a single platform
- ✓ **Comprehensive Threat Visibility**
  Monitor detection coverage delivered by your security tools and our MDR service, mapped to the **MITRE ATT&CK® Framework**
- ✓ **Performance Benchmarking**
  Benchmark team performance, risk posture, and track Median Time to Resolve (**MTTR**) trends
- ✓ **Demonstrate ROI**
  Get visibility into how your current security investments are performing and justify budget requests with Risk-Ranked Reduction Recommendations
- ✓ **Mobile Accessibility**
  Stay connected to all your Critical Start services while on the go with the MOBILE**SOC**® mobile application

A platform approach to Managed Cyber Risk Reduction (MCRR)

Critical Start's cloud-native **Cyber Operations Risk & Response™ platform** is the industry's only technology combining cyber risk monitoring, posture and event analytics, and response orchestration in one platform. The platform provides **24x7x365** visibility into proactive and reactive security, reducing risk through continuous monitoring and expert guidance. Centralized dashboards display Risk Assessments, Asset Visibility, and Managed Detection and Response (**MDR**) in one place for quick insights into your risk posture, detection coverage, and immediate actions.

Reduce the risk of a breach with end-to-end visibility of your security operations

The Cyber Operations Risk & Response™ platform uses APIs to integrate with multiple sources like Entra ID, EDR, EPP, and vulnerability management platforms to quickly identify unprotected assets due to missing or broken endpoint security agents. Additional use cases can include missing vulnerability, patch management, and backup agents. With this visibility, organizations can ensure complete coverage of security controls while providing security operations with additional context to detect and respond to threats. See an actionable view of attacks in progress across your security environment mapped to **MITRE ATT&CK® Framework** and clear, step-by-step response guidance, including asset criticality and where attacks are at in the kill chain.

Prove the value of your existing security operations tools and technology

Align cybersecurity spend to business outcomes using data that articulates the value of your current technology investments. This includes implementing new security programs or improving the maturity of existing programs using quantifiable measurements against your target state and industry peer benchmarks. See which tools and technologies are experiencing problems and which data sources and detections are impacted.

Stay ahead of the latest threats

Critical Start's Start Cyber Research Unit (**CRU**) helps you stay ahead of the latest threats by building, enriching, and adding threat intelligence to your security tools. The Cyber Operations Risk & Response™ platform delivers value through increased visibility into your security posture so your team can view every alert, including alerts automatically resolved, alerts escalated, and the actions we take on your behalf, giving your security team the same view our analysts see.

Features and Capabilities

Cyber Risk Dashboard

The Cyber Risk Dashboard provides a unified view of your organization's risk posture and prioritized recommendations to reduce risk. A pivotal part of the Platform, the Cyber Risk Dashboard offers a holistic perspective for assessing, monitoring, and mitigating your cyber security risk with data-driven insights.

Team Performance Dashboard

The Team Performance Dashboard allows you to measure, analyze, and improve your security team's productivity through key metrics. It assesses performance in critical areas like Median Time to Resolve (**MTTR**) and closed alerts, providing peer comparisons and overall visibility to help your team improve productivity.

MITRE ATT&CK Mitigations Recommendations Report

The MITRE ATT&CK Framework provides awareness of the latest adversary threats and mitigations to protect systems proactively. The MITRE ATT&CK Mitigations Recommendations Report helps you make informed decisions about which defensive measures to enact, fortifying defenses to prevent or deflect an attack in the first place.

The report lists each mitigation's number, name, type, and description and maps it to the corresponding tactics, techniques, and sub-techniques. Mitigations are prioritized by the number of true positive alerts that have occurred in your environment and are correlated to each one, highlighting the highest-impact protections. The report can be generated on demand or scheduled for regular automated delivery.

Trusted Behavior Registry® (TBR®)

The TBR revolutionizes false positive reduction to maximize threat detection. By establishing a baseline of known, trusted system behaviors and filtering normal activity, the TBR ensures analysts can rapidly focus on real threats. The TBR works continuously in the background to separate benign alerts from harmful incidents.

With false positives removed, your security personnel regain the time previously lost on routine alerts. Analyst productivity is boosted by up to 90%, allowing your security team to defend against more impactful attacks through noise reduction and the enablement of human talent.

Endpoint Coverage Gaps

Endpoint Coverage Gaps reveal security blind spots by discovering hosts lacking endpoint protection agents. By mapping all assets and normalizing host data, we identify endpoints operating outside your security controls.

These unprotected hosts represent massive risk exposure due to missing prevention and detection coverage. Endpoint Coverage Gaps shines a light on these gaps to ensure comprehensive monitoring.

SIEM/XDR Health Monitoring

SIEM/XDR Health Monitoring provides centralized observability into the performance of your security data sources. We continuously inspect managed SIEM and XDR tools to identify issues proactively, including Zero-Log Ingest Alerts and log format changes, the primary causes for failed threat detections.

Integrated health tracking spots problems with log data accuracy, availability, or throughput. Detected errors display the impacted sources and detection rules, ensuring a rapid understanding of tooling gaps.

By consolidating health metrics, SIEM/XDR Health Monitoring lets you visualize uptime and reliability while maximizing the value of existing security investments. Unified visibility leads to quicker issue resolution, tighter integrations, and better threat protection.

MobileSOC

Take threat detection and response on the go with our MobileSOC application, a native mobile iOS and Android app that puts the power of the Cyber Operations Risk & Response™ platform in the palm of your hands, allowing you to triage, escalate, and isolate attacks from your phone.

With MobileSOC, you can see the full alert data that we see, communicate directly with Critical Start Risk and Security Operations Center (**RSOC**) senior security analysts, and take immediate action with information gathered by tools and in coordination with your MDR team. Security team leaders also leverage MobileSOC to view operational metrics from their mobile devices – anytime, anywhere.

CRITICALSTART®